COMMENTS OF THE CONSTITUTION PROJECT TO THE REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES

October 30, 2013

Dear Members of the Review Group,

The Constitution Project (TCP) welcomes this opportunity to provide public comments to the Review Group on Intelligence and Communications Technologies (Review Group) as it examines how the United States can use its surveillance authority and technical capabilities in a manner that protects our national security without improperly infringing upon our privacy and civil liberties.

TCP is a non-profit organization that promotes and defends constitutional safeguards and seeks bipartisan solutions to preserve civil liberties. TCP's bipartisan Liberty and Security Committee, launched in the aftermath of September 11th, brings together members of the law enforcement community, legal academics, former government officials, and advocates from across the political spectrum who develop and advance proposals to protect civil liberties as well as our nation's security.

TCP's Liberty and Security Committee has long been engaged in examining the statutory and constitutional questions raised by various government surveillance programs. Our previous analysis and recommendations include a *Statement on Reforming the Patriot Act* in 2009 and a *Report on the FISA Amendment Act* in 2012, in which we set forth in detail the constitutional privacy concerns raised by programmatic surveillance.

On July 9, 2013, TCP participated in a workshop regarding National Security Agency (NSA) surveillance programs hosted by the Privacy and Civil Liberties and Oversight Board (PCLOB), where we offered comments and recommendations in a full statement for the record. Further disclosures since July regarding the NSA's programs and the Foreign Intelligence Surveillance Court's opinions have only strengthened TCP's long-standing position on the need for specific reforms. We restate our recommendations here.

Legal Issues Demanding Reform

1. Likely Violations of Section 215 of the Patriot Act:

The Foreign Intelligence Surveillance Court (FISC) has issued orders under Section 215 of the Patriot Act directing telephone companies to turn over phone records covering millions of Americans to the NSA. Although these orders do not permit the NSA to listen in on calls or obtain their content, the scope of information covered by these orders is staggering. It shows what numbers are calling each other, the duration of these calls, and the frequency with which particular numbers call each other – for all calls, including purely domestic calls between Americans. This information can be highly revealing of the patterns of Americans' associations. But most troubling is the fact that there appears to have been no showing that any of these millions of Americans has any connection to terrorism. Even under the relaxed standards for obtaining Section 215 orders under the Patriot Act, the government is supposed to demonstrate that the information sought is relevant to an investigation to protect against international terrorism or espionage. It is difficult to understand how the phone records of millions of Americans who have not been shown to have any terrorist ties meets this standard of relevance.

The Office of the Director of National Intelligence (ODNI) has defended the program by stating that there are important limits and safeguards being applied. Specifically, the ODNI has announced that the FISC has approved procedures under which the NSA will only "query" the database of phone records when they have "reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization." Under this standard, they report, the call records of fewer than 300 people were actually searched in 2012. But compliance with this "reasonable suspicion" standard is not being assessed by the court – NSA officials apply this rule internally. More importantly, while it may be reassuring to know that the NSA is imposing some internal restraint on its use of this massive database, this restriction does not cure the problem of the initial over-collection of Americans' phone records.

Likely Fourth Amendment Violations Through Both Section 215 and FISA Amendments Act Surveillance:

In addition to the likely violation of Section 215 through the collection of vast amounts of Americans' telephone metadata, this expansive data collection seriously threatens constitutional rights. Although traditionally, courts have not treated such non-content information as being protected by the Fourth Amendment, rapid changes in technology have transformed the nature and extent of this metadata, and the courts are beginning to catch up. Last year, in *United States v. Jones*, the Supreme Court began to recognize that continuous electronic surveillance for an extended period of time implicates the Fourth Amendment. Although the case involved GPS tracking of a car on public roads and the majority decided the case on relatively narrow grounds, the two concurrences in *Jones,* covering a total of five Justices, show that a majority of Justices acknowledge the intrusiveness of powerful electronic surveillance technologies and how continuous use of such technologies over extensive periods of time can impinge on reasonable expectations of privacy. As noted above, with the Section 215 surveillance, the collected data shows what numbers are calling each other, the duration of these calls, and the frequency with

which particular numbers call each other. This information, like the pattern of the car's movements in the *Jones* case, can be highly revealing, including demonstrating the patterns of individuals' daily activities and their associations with others. Such extensive monitoring threatens both First Amendment rights of free association and Fourth Amendment rights to be free from unreasonable searches and seizures.

We have also heard and seen various descriptions of programs such as PRISM that are conducted under the authority of the FISA Amendments Act of 2008. That act amended the Foreign Intelligence Surveillance Act (FISA) to legalize a form of the NSA warrantless wiretapping program disclosed to the public in 2005 and 2006, and it was just reauthorized by Congress in December 2012. The FISA Amendments Act vastly increased the government's powers to conduct surveillance of international communications without individualized judicial review.

Unlike the Section 215 surveillance discussed above, the government *can* collect and review the content of communications under this program, but it is not supposed to collect communications between two U.S. persons (citizens or legal residents) or between two people located within the United States. Thus, when authorized, the collection should cover far fewer Americans than collection under Section 215, since it should only intentionally target international communications.

But the FISA Amendments Act does authorize the government to gather foreign intelligence information through bulk collection of communications. The law does not require the government to identify any particular targets for the surveillance or to provide a rationale for individual targeting decisions. Rather, the government need only provide the FISC with a description of the "targeting" and "minimization" procedures that will be used to decrease the number of U.S. persons whose communications are collected. The departure from traditional Fourth Amendment standards – that searches require warrants based upon a showing of probable cause – is justified by the argument that the targets of programmatic surveillance conducted under the FISA Amendments Act are foreigners located overseas, and thus people who do not have recognized rights under the Fourth Amendment.

To date, we know far less about the legal analysis and operational details supporting surveillance under Section 702 of the FISA Amendments Act programs than about surveillance under Section 215 of the Patriot Act. However, the disclosures in the press have outlined very broad surveillance programs, and if the scope is indeed this extensive, the surveillance likely violates Fourth Amendment rights.

Since enactment of the FISA Amendments Act, we have known that the law would permit the collection of communications in which a U.S. person or someone located within the United States was on the *other end* of a conversation, provided that the target of the collection was indeed a foreigner located abroad. The collection of such communications involving Americans has been described as "incidental," suggesting that it occurs infrequently. The recent disclosures about the PRISM program and other surveillance under the FISA Amendments Act have shown that it is highly misleading to call these collections "incidental." While the disclosures have left many unanswered questions, they have illustrated that the scope and extent of communications collected under these programs is extremely broad and the likelihood that the communications

involve U.S. persons is very high. Moreover, according to newly leaked documents, the standards applied by the NSA in assessing whether communications actually involve a U.S. person, provide the agents with a great deal of discretion to err on the side of assuming that a person is a foreigner and that the communications may be retained and used. They also permit the government to retain and use communications by and about U.S. persons for various purposes even after government agents conclude that they have in fact collected U.S. person information.

Overall, this information indicates that the government is likely collecting the communications – including their content – of vast numbers of Americans. And as a result, the limited review conducted by the FISC under existing law is likely not adequate to protect Americans' Fourth Amendment rights.

2. The Problem of Secret Law:

Above and beyond the likely statutory and constitutional violations that the NSA disclosures have revealed, we must address the problem of "secret law." It should not have taken a leak of classified information for the public to learn how the government has interpreted Section 215 of the Patriot Act. While it may be necessary to maintain secrecy for any *evidence* submitted to the secret Foreign Intelligence Surveillance Court to justify such surveillance, the administration's interpretations of surveillance laws and the standards being applied by the court should be public.

TCP has long called for disclosure of significant opinions of the FISC and other documents showing the administration's interpretations of its authority under the surveillance laws. This will permit meaningful public debate and rigorous oversight of government actions. In addition, in February 2013, TCP's Liberty and Security Committee released its report *Lift the Veil of Secrecy on Targeted Killing*, examining the problem of secret law in the context of the administration's legal analysis regarding the drone or targeted killing program. In that report, TCP's Liberty and Security Committee explained:

> The legal rules and standards under which our government operates should not be secret. While counterterrorism tactics and military strategy may be appropriately withheld from public disclosure, the public has a right to know the legal framework within which these and other operations are conducted, including the safeguards in place to protect constitutional and legal rights. While the president must be able to obtain frank and confidential legal advice about how the law may apply in particular circumstances, the governing rules themselves can never be secret . . .
>
> Our constitutional system of checks and balances demands robust oversight by Congress and consideration and debate by an informed public. Neither is possible when the rules are hidden from Congress and from public view. Sensitive operational and intelligence details may of course remain appropriately classified. But the regime of law and applicable rules that govern national security programs must be made public. Our government's commitment to transparency must not evaporate the moment that national security concerns are invoked.

This analysis applies equally to government surveillance programs. The need for transparency is particularly great where the administration's or the FISC's interpretation of the law is not readily apparent from the text of the statute, such as with the recently revealed interpretation of the scope of Section 215 of the Patriot Act.

The governing law and legal standards under which the administration operates should be public. Secret law has no place in a democracy.

Recommended Reforms:

1. Reforms to Patriot Act Authorities:

Long before recent disclosures outlining NSA surveillance under Section 215 of the Patriot Act, TCP's Liberty and Security Committee had recommended a series of amendments to the Patriot Act to provide more robust protections for civil liberties, as part of its *Statement on Reforming the Patriot Act*. Recent revelations have only made these recommendations more urgent. TCP urges the Review Group to recommend the following reforms at a minimum:

a) Congress should amend the Patriot Act to prohibit bulk collection of communications metadata, through Section 215 or any other surveillance authorities, and should tighten the standards for collection of data under Section 215. This should include all of the following:

i) Tightening the standard for issuing an order under Section 215 to require a showing to a judge of specific and articulable facts demonstrating that the material sought pertains to a suspected agent of a foreign power or a person in contact with or otherwise directly linked to such an agent;

ii) Limiting to 30 days the period during which the recipient of a Section 215 order can be required not to disclose existence of the order, unless the government can prove to a judge that there is reason to believe that a specified and articulable harm would result unless the "gag order" is extended; and

iii) Requiring adoption of minimization procedures, to ensure that the scope of the order is no greater than necessary to accomplish the investigative purpose.

b) Congress should also ensure that broad unchecked surveillance is not simply shifted to another program under another section of the Patriot Act or another statute. This should include enacting reforms to limit the scope of the Patriot Act's national security letter (NSL) authority to bar bulk collection of communications metadata, and:

i) Requiring that NSLs be used only to obtain records that pertain to suspected terrorists or spies, by re-establishing the prior requirement that there be specific and articulable facts giving reason to believe that the records sought pertain to an agent of a foreign power;

ii) Establishing reasonable limits on the "gag" that attaches to an NSL, requiring it to be narrowly tailored and limiting it to 30-days, extendable only by a court and based upon a showing of necessity;

iii) Establishing recipients' rights to seek judicial review of NSLs; and

iv) Requiring adoption of minimization procedures for information obtained with an NSL to ensure that the scope of the order is no greater than necessary to accomplish the investigative purpose.

2. Reforms to FISA Amendments Act Authorities:

Similarly, well before recent disclosures regarding the scope of collection programs under the FISA Amendments Act, TCP's Liberty and Security Committee had recommended a series of amendments to the FISA Amendments Act to provide more robust protections for civil liberties, as part of its *Report on the FISA Amendment Act*. That report focused on two problems: the need for more rigorous review by the FISC before surveillance is authorized and the need for safeguards to protect U.S. person information post-collection. Recent revelations about NSA surveillance have highlighted the need for both categories of safeguards. Thus, TCP urges the Review Group to recommend the following reforms at a minimum:

a) Increased Judicial Review of Surveillance Authorizations: The FISA Amendments Act should be amended to require more robust judicial review by the FISC to authorize programmatic surveillance and ensure that it is appropriately focused on foreign intelligence. Specifically:

i) Congress should restore the requirement that foreign intelligence be the primary purpose of the programmatic surveillance.

ii) When seeking approval for programmatic surveillance, the government should be required to (1) explain the foreign intelligence purpose of the proposed surveillance, (2) define the scope of planned interceptions, and (3) provide a risk assessment and an estimate of reasonably anticipated interceptions of the communications of U.S. persons and individuals located within the United States. The surveillance should only be permitted after the FISC has thoroughly evaluated these submissions to ensure that surveillance is appropriately designed to acquire foreign intelligence information from legitimate targets without interfering with the privacy rights of U.S. persons and individuals located within the United States.

iii) Additionally, the government should be required to develop and submit to the FISC procedures for determining when an acquisition may be expected to collect communications to or from the United States. Then, in cases where the planned surveillance may reasonably be expected to intercept communications to or from a person reasonably believed to be in the United States, the government should be required to obtain a FISA warrant under pre-FISA Amendments Act standards.

b) Inclusion of Warrant Requirements and Other Safeguards for Post-Collection Use of Information: The FISA Amendments Act should be amended to require that the government obtain a warrant from the FISC before searching collected communications for information on a specific U.S. person, decrypting the identity of a specific U.S. person party to a conversation, or reviewing communications reasonably believed to be to or from the United States. As required under the pre-FISA Amendments Act version of FISA, the warrant should be based upon a showing of probable cause to believe that the target is an agent of a foreign power or has committed a crime, and that evidence of the crime will be found and must name its target(s) with particularity.

Moreover, Congress should ensure that collected information is being properly used for foreign intelligence purposes, including at the very least a requirement that authorities obtain a warrant before using data for law enforcement purposes. Finally, Congress should amend the FISA Amendments Act to require more stringent procedures for minimization, including periodic, ongoing FISC review of the implementation and efficacy of such procedures.

3. Reforms to Promote Transparency:

Perhaps most importantly, the Review Group can recommend an end to the vast body of "secret law," a move that would bring much needed transparency to government surveillance programs. As discussed above, although sensitive operational details about surveillance programs will need to remain classified, the government's interpretations of statutes and the applicable legal rules that govern national security programs must be made public. The Review Group's mandate specifically recognizes the "need to maintain the public trust." In recent months, much of that public trust has eroded. Ending secret law is a necessary first step to regaining it.

In particular, TCP urges that the Review Group recommend that:

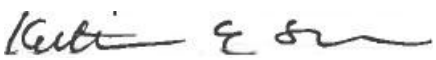
a) More information about the intelligence community's use of the FISA Amendments Act should be provided to Congress, the Privacy and Civil Liberties Oversight Board, and the public.

b) The Inspector General of the Intelligence Community should be required to audit these surveillance programs under the FISA Amendments Act and issue annual reports to Congress regarding how government surveillance has been conducted. In particular, these reports should include: statistics regarding how many U.S. persons' communications have been intercepted by the government; aggregate statistics on the number of intercepted communications in total, and the number of intercepted communications to or from the United States or involving any U.S. person; an analysis of the performance of the government's targeting and minimization procedures; and an explanation of how collected information has been used, including the number of times the information has been used for law enforcement rather than foreign intelligence purposes. These reports should also be provided in an unclassified form released to the public. Additionally, as much as practicable, more information on the FISA Amendments Act should be released to the public, including important decisions by the FISC and Foreign Intelligence Surveillance Court of Review, redacted as necessary.

c) The Review Group should further urge disclosure of other information necessary for public understanding of the scope of surveillance authorities, safeguards for privacy rights and civil liberties, and the historical development of the law since 2001.

Respectfully submitted,

Virginia E. Sloan
President



Katherine E. Stern
Senior Counsel, Rule of Law Program